Załącznik Nr 7
do Zarządzenia Nr 10 /2015
Burmistrza Miasta i Gminy Stopnica
z dnia 19 stycznia 2015 r.

System służący ochronie danych, w tym: dowodów księgowych, ksiąg rachunkowych i innych dokumentów stanowiących podstawę dokonanych w nich zapisów w Urzędzie Miasta i Gminy Stopnica

Zasady ochrony danych.

Programy stosowane w jednostce ograniczają dostęp do danych, w tym: do dowodów księgowych, ksiąg rachunkowych i innych dokumentów finansowych, między innymi poprzez konieczność podania hasła w momencie uruchamiania systemu. Hasła te są przypisane konkretnemu użytkownikowi i zmieniane są okresowo. Podczas wpisywania nie pojawia się ono na ekranie. Ma to na celu zabezpieczenie przed podpatrzeniem go przez osoby postronne.

Nierozerwalnie z symbolem użytkownika i hasłem wiąże się problem ograniczenia dostępu do

niektórych funkcji systemu. Przy instalacji systemu zakodowano ilość użytkowników, nadano im hasła oraz określono dostępność funkcji dla każdego z nich. Dotyczy to zarówno funkcji ogólnych znajdujących się na najwyższym "poziomie" systemu w tzw. menu, jak i tych najbardziej szczegółowych przypisanych do poszczególnych elementów okna tzw. komponentów. System blokowania dostępu przydatny jest zwłaszcza w odniesieniu do funkcji niosących z sobą, jeśli są wykonane w nieodpowiednim momencie lub przez nieodpowiedzialnego operatora, niebezpieczeństwo utraty danych (np. zamykanie miesiąca itp.). Z punktu widzenia zakresu posiadanych uprawnień dzieli się użytkowników na dwie grupy: aktywnych i biernych. Status "aktywnego" pozwala na pełną obsługę dostępnych funkcji, natomiast użytkownik "bierny" nie ma możliwości ingerencji w bazy danych pomimo formalnej dostępności do określonych funkcji systemu.

Oznacza to w praktyce, że osoby uprawnione do wykonywania tych samych funkcji programu różnią się zakresem dostępnych działań. Np. jedna z nich może zarówno dopisywać pozycje do katalogu kontrahentów lub korygować zawartość już istniejących, a druga tylko korygować dane, przy czym obie pozbawione są prawa do usuwania pozycji.

Generalnie operację kodowania dostępu do systemu dokonuje osoba instalująca i wdrażająca

program. Dla użytkowników zainteresowanych samodzielną obsługą uprawnień, co jest uzasadnione zwłaszcza w przypadku pracy sieciowej, producenci dostarczyli programy kodujące (np. ADMIN w programie Puma) wraz z odpowiednim opisem.

Jeśli podane hasło było prawidłowe następuje sprawdzenie czy użytkownik o danym kodzie już nie pracuje w systemie.

Równolegle z ograniczeniami programowymi administrator systemu może sterować dostępem do systemu za pomocą mechanizmów zawartych w stosowanym oprogramowaniu sieciowym.

Istotnym elementem składowym systemu informatycznego rachunkowości jest dokumentacja eksploatacyjna (czasami nazywana również dokumentacją użytkownika). Instrukcja dostarczana każdorazowo z każdym systemem (oprogramowaniem) ma spełniać rolę takiej dokumentacji. Zawiera ona informację zapoznające użytkownika z:

-zakresem i funkcjami realizowanymi przez system,

-algorytmami przetwarzania danych

-zestawem informacji możliwych do otrzymania za pośrednictwem systemu,

-zasadami ochrony danych,

-powiązaniami między podsystemami rachunkowości i systemami współpracującymi z systemem FK,

-zasadami organizacji procesu wdrożenia systemu i jego bieżącej eksploatacji.

Ochrona danych

W programach księgowych stosowanych w urzędzie oprócz standardowych mechanizmów ochrony danych (hasła dostępu, ograniczanie uprawnień do poszczególnych funkcji systemu, kopie danych) zastosowano dwa mechanizmy typowe dla tego systemu:

1. Ogólne ograniczenie dostępu użytkownikom do danych. Istnieje zatem konieczność świadomego nadania uprawnień dla konkretnego użytkownika do danych wybranego dysponenta (dysponentów) budżetowych;
2. Ewidencjonowanie zmian w dokumentach (kto, kiedy, rodzaj zmiany).

Pierwszy z mechanizmów polegający na ogólnym ograniczeniu dostępu do danych objawia się tym, że domyślnie nowy użytkownik nie ma dostępu do żadnych danych. Konieczne jest wskazanie przez administratora systemu jaki zakres danych ma być dla tego użytkownika dostępny. Do systemu wbudowana została więc funkcja (dostępna tylko i wyłącznie dla Administratora) przypisywania użytkownikowi tych symboli dysponentów (wydziałów) budżetowych, za których dane odpowiada. Po takim przypisaniu kontrola dostępu sprawdzana jest systemowo na wszystkich poziomach poprzez odpowiednie filtrowanie danych. Po zalogowaniu się do systemu użytkownik we wszystkich kartotekach, zestawieniach, analizach przegląda wyłącznie dokumenty dotyczące udostępnionych mu dysponentów.

Drugi z mechanizmów polega na ewidencjonowaniu każdej zmiany, jaka nastąpiła w

dokumentach budżetowych. Zapisywane są informacje o tym kto (kod użytkownika) i kiedy (data – rok, miesiąc, dzień;) określony dokument wprowadził.

Tak więc uruchomienie programu i dostęp do danych zapisanych w systemie chroniony jest systemem kodów, haseł i uprawnień. W systemie przewidziane są trzy stopnie uprawnień:

-uprawnienia pozwalające tylko na przeglądanie danych,

-uprawnienia pozwalające na zapisy w bazie danych; w przypadku dekretacji i księgowania dotyczy to tylko modyfikacji i księgowania zapisów autora, czyli osoby, która wprowadziła dany dekret,

-uprawnienia administratora modułu pozwalające na wykonanie wszystkich operacji z korektą i księgowaniem „obcych" dekretów włącznie.

Kody i uprawnienia osobom upoważnionym nadaje administrator systemu.

Wszystkie zapisy w systemie zawierają dane informujące o tym kto i kiedy dokonał zapisu.

Nad bezpieczeństwem programu czuwa administrator programu.

Do zadań administratora (informatyka) należy:

a.) ewidencjonowanie osób uprawnionych do korzystania z programu – nadawanie kodów i uprawnień poszczególnym operatorom programu.

b.) ustalenie częstotliwości zmiany haseł.

c.) wykonanie i zabezpieczenie kopii bazy danych.

Oprócz zabezpieczeń dostępu do pracy z programem dane chronione są poprzez zamykanie okresów sprawozdawczych.

Okresem sprawozdawczym w programie jest miesiąc obrachunkowy. Po zaksięgowaniu wszystkich operacji księgowych danego miesiąca i zatwierdzeniu sprawozdań należy miesiąc zamknąć. Do zamkniętego miesiąca nie można księgować żadnych operacji, nie można zmienić stanów kont. W ten sposób zapewniona jest spójność pomiędzy sprawozdaniami i danymi księgowymi.

Jeżeli zachodzi konieczność skorygowania danych z zamkniętego miesiąca można skorygować stany kont narastająco w miesiącu następnym po zamkniętym okresie sprawozdawczym.

Korygowanie danych księgowych możliwe jest tylko na etapie dokumentów nie zaksięgowanych. Po zaksięgowaniu dokumentu korekta możliwa jest tylko poprzez zaksięgowanie dokumentu korygującego (PK).

Usuwanie kont z planu kont dotyczy tylko kont nie czynnych tzn. kont na których nie były rejestrowane żadne operacje księgowe. Konto nie może być usunięte, jeżeli były zaksięgowane operacje, nawet jeżeli konto wykazuje saldo zerowe.

Ochroną danych objęte są: księgi rachunkowe, księgi kontowe, wydruki komputerowe, dowody księgowe, dokumenty inwentaryzacyjne, inne dokumenty księgowe oraz sprawozdania finansowe.

W celu zapewnienia ochrony danych tworzy się komputerowe kopie operacji gospodarczych na dysku twardym.

Codziennie wykonywana jest automatyczna kopia bazy danych na serwerze zakupionym w ramach projektu e-świętokrzyskie, znajdującym się w wyznaczonym pomieszczeniu Urzędu Miasta i Gminy przez informatyka urzędu. Kopia z przeprowadzonej archiwizacji danych zapisywana jest automatycznie dodatkowo w drugiej lokalizacji czyli na serwerze Windows 2003, znajdującym się w innym pomieszczeniu Urzędu Gminy.

Dodatkowo raz na m-c informatyk zobowiązany jest do dokonywania zapisu wykonanych kopii bazy danych na płytach DVD.

W urzędzie, w budynku na Wolicy, gdzie prowadzona jest ewidencja analityczna i rozliczenia wpłat za wodę i ścieki a także wystawiane są faktury sprzedaży i prowadzone rejestry VAT rezerwowa kopia zbioru danych ksiąg rachunkowych oraz dokumentów księgowych wykonywana jest systematycznie czyli codziennie po zakończonej pracy przez pracownika na dysku twardym komputera, w specjalnie utworzonym folderze oraz dodatkowo zapisywana jest na przenośnym urządzeniu -nośniku danych – Pendrive. Na koniec każdego m-ca kopia bazy danych zapisywana jest na płycie DVD.

Zbiory danych sporządzane są również w wersji papierowej.

W celu zapewnienia należytej ochrony programów i zawartych w nich danych stosuje się na każdym stanowisku komputerowym indywidualne hasła użytkowników systemu, chroniące przed dostępem osób nieupoważnionych.

W celu ochrony danych i ich zbiorów przed możliwością całkowitej lub częściowej utraty w wyniku różnych nieprzewidzianych zdarzeń wprowadza się jako obowiązujące niżej podane zasady do ścisłego przestrzegania:

– od kradzieży sprzętu komputerowego; pomieszczenie, w którym znajduje się komputer zawierający chronione dane musi być zamykane w okresie, gdy nie przebywa w nim żaden z pracowników oraz odpowiednio zabezpieczone przed możliwością włamania,
– od całkowitego zniszczenia sprzętu komputerowego w wyniku pożaru, zalania lub innych zdarzeń losowych; przechowywanie zapasowych kopii danych i programu instalacyjnego powinno być zgodne z wyżej ustalonymi zasadami; obowiązuje też zapewnienie nadzoru nad pomieszczeniami Urzędu poza godzinami pracy.